

## **CLAIM AMENDMENTS**

### **Claim Amendment Summary**

#### **Claims pending**

- Before this Amendment: Claims 1-36
- After this Amendment: Claims 1-36.

**Non-Elected, Canceled, or Withdrawn claims:** 28.

**Amended claims:** 1, 10, 20, and 29-30.

**New claims:** None.

---

### **Claims:**

**1. (Currently Amended)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs acts comprising:

obtaining two input polynomials each with degree  $[\leq] 5$ , wherein a first polynomial is nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and a second polynomial is nominally described as  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$  and terms  $a_5$  and  $b_5$  are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen;

reporting results of the computing.

**2. (Original)** A medium as recited in claim 1 further comprising repeating the obtaining and the computing.

**3. (Original)** A medium as recited in claim 1 further comprising:  
selecting a pair of polynomials from a collection of pairs and providing the selected polynomials to the obtaining;  
repeating the selecting, obtaining, and computing.

4. **(Original)** A medium as recited in claim 1, wherein during the computing, calculating:

$$\begin{aligned}
 & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
 & + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
 & + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
 & + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - \\
 & X^3) \\
 & + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
 & + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
 & + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
 & ^2) \\
 & + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
 & ^3) \\
 & + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
 & + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
 & + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
 & + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
 & + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
 & + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
 & + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
 & + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
 & + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
 & + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
 \end{aligned}$$

to compute the product polynomial, where  $C$  is a polynomial constant value and the two input polynomials are nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ , respectively.

**5. (Original)** A medium as recited in claim 4, wherein the variable  $X$  is replaced by its negative ( $-X$ ) and the odd-indexed coefficients,  $a_1, a_3, a_5, b_1, b_3, b_5$ , are replaced by their negatives.

**6. (Original)** A medium as recited in claim 4, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

**7. (Original)** A medium as recited in claim 4, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or  $-1$ .

**8. (Original)** A medium as recited in claim 1, wherein the two input polynomials are representative of integers, which are nominally labeled:  $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$  and  $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$ , respectively, where  $0 \leq a_i < R$  and  $0 \leq b_j < R$ .

9. **(Original)** A medium as recited in claim 8, wherein  $j$  is  $\geq 0$  and  $\leq$   
5.

10. **(Currently Amended)** A computing device comprising:  
an audio/visual output ;  
a ~~[medium as recited in claim 1]~~ computer-readable medium having  
computer-executable instructions that, when executed by a computer, performs  
acts comprising:

obtaining two input polynomials each with degree  $[\leq] 5$ ,  
wherein a first polynomial is nominally described as  $a(X) = a_0 + a_1X$   
 $+ a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and a second polynomial is nominally  
described as  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$  and  
terms  $a_5$  and  $b_5$  are non-zero values;

computing a product polynomial of the input polynomials,  
wherein the total number of coefficient multiplication operations is  
fewer than or equal to seventeen;

reporting results of the computing.

**11. (Original)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining two input polynomials each with degree  $\leq 5$  ;

computing a product polynomial of the input polynomials, wherein such computing comprises calculating:

$$\begin{aligned}
 & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
 & + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
 & + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
 & + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - \\
 & X^3) \\
 & + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
 & + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
 & + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
 & ^2) \\
 & + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
 & ^3) \\
 & + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
 & + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
 & + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
 & + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
 & + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
 & + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
 & + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1)
 \end{aligned}$$

$$\begin{aligned}
&+ a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
&+ a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
&+ a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
\end{aligned}$$

to compute the product polynomial, where  $C$  is a constant value and the two input polynomials are nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ , respectively; reporting results of the computing.

**12. (Original)** A medium as recited in claim 11, wherein the variable  $X$  is replaced by its negative ( $-X$ ) and the odd-indexed coefficients,  $a_1, a_3, a_5, b_1, b_3, b_5$ , are replaced by their negatives.

**13. (Original)** A medium as recited in claim 11, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

**14. (Original)** A medium as recited in claim 11, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or  $-1$ .

**15. (Original)** A medium as recited in claim 11 further comprising repeating the obtaining and the computing.

- 16. (Original)** A medium as recited in claim 11 further comprising:  
selecting a pair of polynomials from a collection of one or more pairs of polynomials and providing the selected polynomials to the obtaining;  
repeating the selecting, obtaining, and computing.
- 17. (Original)** A medium as recited in claim 11, wherein the total number of coefficient multiplication operations performed during the computing is fewer than or equal to seventeen.
- 18. (Original)** A medium as recited in claim 11, wherein the two input polynomials are representative of integers base  $R$  and a length  $n$  and wherein  $X = R$  in the calculating.
- 19. (Original)** A medium as recited in claim 11, wherein  $C$  is zero.



**20. (Currently Amended)** A method comprising:

obtaining two input polynomials with six terms each, wherein a first polynomial is nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and a second polynomial is nominally described as  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$  and terms  $a_5$  and  $b_5$  are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen;

reporting results of the computing.

**21. (Original)** A method as recited in claim 20 further comprising repeating the obtaining and the computing.

**22. (Original)** A method as recited in claim 20 further comprising:

selecting a pair of polynomials from a collection of one or more pairs of polynomials and providing the selected polynomials to the obtaining;

repeating the selecting, obtaining, and computing.

**23. (Original)** A method as recited in claim 20, wherein during the computing, calculating:

$$\begin{aligned}
 & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
 & + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
 & + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
 & + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - \\
 & X^3) \\
 & + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
 & + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
 & + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
 & ^2) \\
 & + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
 & ^3) \\
 & + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
 & + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
 & + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
 & + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
 & + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
 & + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
 & + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
 & + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
 & + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
 & + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
 \end{aligned}$$

to compute the product polynomial, where  $C$  is a polynomial constant value and the two input polynomials are nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ , respectively.

**24. (Original)** A method as recited in claim 23, wherein the variable  $X$  is replaced by its negative ( $-X$ ) and the odd-indexed coefficients,  $a_1, a_3, a_5, b_1, b_3, b_5$ , are replaced by their negatives.

**25. (Original)** A method as recited in claim 23, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

**26. (Original)** A method as recited in claim 23, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or  $-1$ .

**27. (Original)** A method as recited in claim 20, wherein the two input polynomials are representative of integers, which are nominally labeled:  $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$  and  $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$ , respectively, where  $0 \leq a_i < R$  and  $0 \leq b_j < R$ .

**28. (Canceled)**

**29. (Currently Amended)** A system facilitating cryptographic security, the system comprising:

a memory comprising a set of computer program instructions; and

a processor coupled to the memory, the processor being configured to execute the computer program instructions, which comprise:

obtaining two input polynomials with six terms each, wherein a first polynomial is nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and a second polynomial is nominally described as  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$  and terms  $a_5$  and  $b_5$  are non-zero values;

computing a product polynomial of the input polynomials, wherein the total number of coefficient multiplication operations is fewer than or equal to seventeen;

reporting results of the computing.

**30. (Currently Amended)** A system as recited in claim 29, wherein during the computing, the computer program instructions further comprise calculating:

$$\begin{aligned}
 & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) C \\
 & + (a_1 + a_2 + a_4 + a_5) (b_1 + b_2 + b_4 + b_5) (-C + X^6) \\
 & + (a_0 + a_1 + a_3 + a_4) (b_0 + b_1 + b_3 + b_4) (-C + X^4) \\
 & + (a_0 - a_2 - a_3 + a_5) (b_0 - b_2 - b_3 + b_5) (C - X^7 + X^6 - X^5 + X^4 - \\
 & X^3) \\
 & + (a_0 - a_2 - a_5) (b_0 - b_2 - b_5) (C - X^5 + X^4 - X^3) \\
 & + (a_0 + a_3 - a_5) (b_0 + b_3 - b_5) (C - X^7 + X^6 - X^5) \\
 & + (a_0 + a_1 + a_2) (b_0 + b_1 + b_2) (C - X^7 + X^6 - 2X^5 + 2X^4 - 2X^3 + X \\
 & ^2) \\
 & + (a_3 + a_4 + a_5) (b_3 + b_4 + b_5) (C + X^8 - 2X^7 + 2X^6 - 2X^5 + X^4 - X \\
 & ^3) \\
 & + (a_2 + a_3) (b_2 + b_3) (-2C + X^7 - X^6 + 2X^5 - X^4 + X^3) \\
 & + (a_1 - a_4) (b_1 - b_4) (-C + X^4 - X^5 + X^6) \\
 & + (a_1 + a_2) (b_1 + b_2) (-C + X^7 - 2X^6 + 2X^5 - 2X^4 + 3X^3 - X^2) \\
 & + (a_3 + a_4) (b_3 + b_4) (-C - X^8 + 3X^7 - 2X^6 + 2X^5 - 2X^4 + X^3) \\
 & + (a_0 + a_1) (b_0 + b_1) (-C + X^7 - X^6 + 2X^5 - 3X^4 + 2X^3 - X^2 + X) \\
 & + (a_4 + a_5) (b_4 + b_5) (-C + X^9 - X^8 + 2X^7 - 3X^6 + 2X^5 - X^4 + X^3) \\
 & + a_0 b_0 (-3C + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3 - X + 1) \\
 & + a_1 b_1 (3C - X^7 - X^5 + X^4 - 3X^3 + 2X^2 - X) \\
 & + a_4 b_4 (3C - X^9 + 2X^8 - 3X^7 + X^6 - X^5 - X^3) \\
 & + a_5 b_5 (-3C + X^{10} - X^9 + 2X^7 - 2X^6 + 3X^5 - 2X^4 + 2X^3)
 \end{aligned}$$

to compute the product polynomial, where  $C$  is a polynomial constant value [and the two input polynomials are nominally described as  $a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$  and  $b(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4 + b_5X^5$ , respectively].

**31. (Original)** A system as recited in claim 30, wherein the variable  $X$  is replaced by its negative ( $-X$ ) and the odd-indexed coefficients,  $a_1, a_3, a_5, b_1, b_3, b_5$ , are replaced by their negatives.

**32. (Original)** A system as recited in claim 30, wherein the computing is performed in a finite field of characteristic 2, with each even coefficient replaced by zero and each odd coefficient replaced by one.

**33. (Original)** A system as recited in claim 30, wherein the computing is performed in a finite field of characteristic 3, with each coefficient in claim 4 replaced by its modulo 3 image 0, 1 or  $-1$ .

**34. (Original)** A system as recited in claim 29, wherein the two input polynomials are representative of integers, which are nominally labeled:  
 $A = a(R) = \sum_{0 \leq i \leq n-1} a_i R^i$  and  $B = b(R) = \sum_{0 \leq j \leq n-1} b_j R^j$ , respectively, where  $0 \leq a_i < R$  and  $0 \leq b_j < R$ .

**35. (Original)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs acts comprising:

obtaining two input polynomials each with degree  $\leq n$ , where  $n$  is a positive integer;

computing a product polynomial of the input polynomials, wherein the computing has an asymptotic cost is  $n^c$  for  $c$  with  $1 < c < \log(3)/\log(2)$ ;

reporting results of the computing.

**36. (Original)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs acts comprising:

obtaining two input polynomials each with degree  $\leq n$ , where  $n$  is a positive integer;

computing a product polynomial of the input polynomials, wherein the computing has an asymptotic cost is  $n^c$  for  $c = \log(17)/\log(6)$ ;

reporting results of the computing.